# Challenges in Data Privacy and Security

- **Data Sensitivity and Privacy Risks**

Handling personal or sensitive data increases the risk of misuse or exposure if not properly protected.

- **Data Breaches and Unauthorized Access**

Storing AI models and data in the cloud environment makes them vulnerable to cyber threats.

- **Lack of Transparency and Explainability**

Many AI systems operate as black boxes, making it difficult to understand how decisions are made. So they fail to gain public acceptance.

# Privacy Preserving Techniques for AI

- **Differential Privacy**

Differential Privacy is a technique that adds random noise to data or results. It protects individual information while still allowing useful insights from the whole dataset.

- **Federated Learning**

Its a decentralized learning method where many local devices train a model using their own data. Only the updated model parts are sent to a central device, which combines them to improve the shared model.

- **Homomorphic Encryption**

Homomorphic Encryption lets you do calculations on encrypted data without decrypting it. This keeps sensitive info, like medical or financial records, private while still allowing AI to analyze it securely

- **Secure Multi-Party Computation (SMPC)**

Secure Multi-Party Computation lets different parties work together to compute something using their private data, but no one sees each other's raw data. They use encrypted or secret-shared pieces to do this safely. For example, banks can find common fraud patterns without sharing customer details.

# What methods are suitable for our project?

- **Face Region Masking or Partial Obfuscation**

Only retain regions critical for signal extraction (e.g., forehead, cheeks).
Mask or blur the rest of the face.
– Prevents reconstruction or recognition of the full identity

- **Store Only Derived Signals, Not Raw Videos**

Extract signals (e.g., blood pressure, $SpO_2$) immediately and discard the raw video after processing.
– No facial videos remain after processing, eliminating risk of re-identification

# What methods are suitable for our project?

- **Use On-Device Processing**

Perform signal extraction directly on edge devices (e.g., mobile phone)

- Sensitive data never leaves the device.
- Protects against server side breaches.

- **Face Template Hashing**

If any facial features (e.g., landmarks, embeddings) are stored, hash or encrypt them

- Reverse engineering back to a recognizable face becomes difficult.